Wellington, Fla., Breach Larger than Initially Thought

June 14, 2018

(TNS) — Wellington, Fla., Chief information officer William Silliman also said the breach began as an effort to mine for the digital currency Bitcoin, but at some point expanded to include a sophisticated “skimmer” to capture credit card numbers.

In a news release last week, Wellington warned that utility customers who made one-time debit or credit card payments between July 2017 and the beginning of this month may have had their credit card numbers stolen as part of the breach.

But one-time debit or credit card payments made to the village’s code, building, business licenses, parking tickets and planning departments also were exposed, Silliman said, citing the results of further assessment of the targeted server.

Other forms of payment — including e-checks and payments made over the phone — were not affected, and credit card numbers that were set up to pay automatically should be safe, Silliman said.

The system now is safe to use, officials said.

The breach did not target Wellington specifically, but rather set its sights on the Click2Gov vendor the village uses to collect online payments. Superion, the software’s creator, notified Wellington at 2 p.m. June 6 that its servers may have been exposed, and within an hour, the decision was made to shut down the system, Silliman said.

Wellington isn’t the first municipality to suffer a breach of its Click2Gov system. Numerous communities across the U.S. have reported a similar issue. Lake Worth said in February a breach of its Click2Gov system had left its customers exposed, and two California communities reported similar breaches in February and May.

To better understand the breach, Silliman and his team are working with the Sylint Group, a data breach specialist that has worked with other communities where Click2Gov information has been exposed.

In Wellington’s case, the hackers switched the server into a mode that made the real code invisible, then layered their Bitcoin-mining and credit card-skimming code on top of that. The code would collect batches of credit card numbers, encrypt them and ship them to parts unknown. Then the code would “clean up after itself,” Silliman said. “It was really well-written and, this is Sylint’s term, specifically written for Click2Gov.”

Once Wellington knew the potential severity of the breach, it began building new virtual servers to host its billing system. The new servers have added layers of security beyond what previously existed, Silliman said, declining to elaborate publicly.

There was some hint of Click2Gov’s issues beginning last year, when Wellington received an email from Superion in September and another in October, saying some vulnerabilities were possible. Silliman’s team in both cases followed the steps to take care of any issues. Another notification arrived in April, and Wellington followed the same process.

Council members and Silliman expressed frustration with Superion, questioning what the company knew and when.

While Superion did not answer specific questions for this article, a spokeswoman did send a statement: “Protecting our customers and their clients’ data is of the utmost importance to Superion,” she wrote. “Last year, we reported that a limited number of on-premise clients’ networks were compromised. We continue to investigate any suspicious activity and have engaged a leading forensic investigation firm to assist in our efforts. We notified Superion customers of this incident, including the Village of Wellington, and are working closely with our customers to swiftly resolve and remediate this matter.”

http://www.govtech.com/security/Wellington-Fla-Breach-Larger-than-Initially-Thought.html